SECTION I—CLAIMS

Amendment to the Claims:

This listing of the claims will replace all prior versions and listings of claims in the application. Claims 26-30, 32, 34-38, and 40-43 are amended herein. Claims 1-25 remain canceled herein without prejudice. New claim 45 is presented herein. Claims 26-45 remain pending in the application.

Listing of Claims:

1-25. (Canceled).

26. (Currently amended) A method in a packet forwarder, comprising:

receiving a connection request from an unauthorized computing device at a first port of the packet forwarder, the unauthorized computing device requesting access to a network communicably interfaced with a second port of the packet forwarder;

blocking all data packets received at the first port of the packet forwarder from accessing the network;

issuing the unauthorized computing device a first Internet Protocol (IP) address assigned to a first Virtual Local Area Network (VLAN) ~~communicably interfaced with~~ operating within the packet forwarder and associated with the first port, wherein the first VLAN does not provide access to the network communicably interfaced with the packet forwarder via the second port, and wherein the packet forwarder blocks the data packets in the first VLAN from reaching ~~and is isolated from~~ a permanent VLAN that provides access to the network, the permanent VLAN operating within the network and associated with the second port of the packet forwarder and not the first port of the packet forwarder;

sending the unauthorized computing device an authentication request through the first port of the packet forwarder via the first VLAN based on the first IP address, responsive to the connection request;

authorizing the computing device based on satisfactory ~~receiving~~ authentication credentials received from the computing device through the first port of the packet forwarder via the first VLAN, responsive to the authentication request;

issuing the authorized computing device a replacement IP address assigned to the permanent VLAN for communication with the network and associating the first port of the network forwarder with the permanent VLAN; and ~~, responsive to receiving satisfactory authentication credentials from the computing device; and~~

forwarding ~~network~~ the data packets ~~between the~~ received from the authorized computing device at the first port of the packet forwarder to ~~and~~ the network via the second port of the packet forwarder using ~~over~~ the permanent VLAN based on the replacement IP address assigned to the authorized computing device.

27. (Currently amended) The method of claim 26, wherein receiving the connection request from the unauthorized computing device requesting access to the network comprises:

intercepting a request from the unauthorized computing device for a web page.

28. (Currently amended) The method of claim 26, wherein sending the unauthorized computing device the authentication request comprises:

directing the unauthorized computing device to a network login page for authentication, the network login page accessible on the first VLAN.

29. (Currently amended) The method of claim 28, wherein authorizing the computing device based on satisfactory ~~receiving the~~ authentication credentials from the computing device via the first VLAN, responsive to the authentication request comprises:

receiving at least a user name and a password from the unauthorized computing device based on information captured by the network login page.

30. (Currently amended) The method of claim 28, wherein directing the unauthorized computing device to the network login page for authentication comprises:

responding to the unauthorized computing device with a redirect to a Uniform Resource Locator (URL) address for the network login page.

31. (Previously presented) The method of claim 26, further comprising:

sending the authentication credentials to an authentication server; and

receiving an indication from the authentication server that the authentication credentials are authentic and that a user associated with the authentication credentials is authorized to access the network.

32. (Currently amended) The method of claim 31, wherein sending the authentication credentials to the authentication server comprises:

creating a packet comprising the authentication credentials in accordance with a Remote Authentication Dial-In User Service (RADIUS) communications protocol; and

forwarding the packet to a RADIUS server for authentication, wherein the RADIUS server is accessible from the first VLAN.

33. (Previously presented) The method of claim 26, wherein the packet forwarder comprises a switch device located at an edge of the network to provide packet-forwarding services into the network.

34. (Currently amended) The method of claim 26, further comprising:

terminating forwarding of the ~~network~~ data packets between the authorized computing device and the network based on one or more events including:

exceeding a pre-determined period of inactivity by the authorized computing device;

receiving a reset signal is from a network login controller communicably interfaced with the packet forwarder;

receiving a termination command from an administrator account requesting forwarding of the ~~network~~ data packets between the authorized computing device and the network be terminated;

determining a network connection between the authorized computing device and the packet forwarder is disconnected; and

determining a user of the authorized computing device has logged off of the computing device.

35. (Currently amended) A computer-readable medium having instructions stored thereon that, when executed by a processor, cause the processor to perform a method comprising:

receiving a connection request from an unauthorized computing device at a first port of a packet forwarder, the unauthorized computing device requesting access to a network communicably interfaced with a second port of the packet forwarder;

blocking all data packets received at the first port of the packet forwarder from accessing the network;

issuing the unauthorized computing device a first Internet Protocol (IP) address assigned to a first Virtual Local Area Network (VLAN) ~~communicably interfaced with~~ operating within the packet forwarder and associated with the first port, wherein the first VLAN does not provide access to the network communicably interfaced with the packet forwarder via the second port, and wherein the packet forwarder blocks the data packets in the first VLAN from reaching ~~and is isolated from~~ a permanent VLAN that provides access to the network, the permanent VLAN operating within the network and associated with the second port of the packet forwarder and not the first port of the packet forwarder;

sending the unauthorized computing device an authentication request through the first port of the packet forwarder via the first VLAN based on the first IP address, responsive to the connection request;

authorizing the computing device based on satisfactory ~~receiving~~ authentication credentials received from the computing device through the first port of the packet forwarder via the first VLAN, responsive to the authentication request;

issuing the authorized computing device a replacement IP address assigned to the permanent VLAN for communication with the network and associating the first port of the network forwarder with the permanent VLAN; and ~~, responsive to receiving satisfactory authentication credentials from the computing device; and~~

forwarding ~~network~~ the data packets ~~between the~~ received from the authorized computing device at the first port of the packet forwarder to ~~and~~ the network via the second port of the packet forwarder using ~~over~~ the permanent VLAN based on the replacement IP address assigned to the authorized computing device.

36. (Currently amended) The computer-readable medium of claim 35, wherein receiving the connection request from the unauthorized computing device requesting access to the network comprises:

intercepting a request from the unauthorized computing device for a web page.

37. (Currently amended) The computer-readable medium of claim 35, wherein:

sending the unauthorized computing device the authentication request comprises directing the computing device to a network login page for authentication, the network login page accessible on the first VLAN; and wherein

receiving the authentication credentials from the unauthorized computing device via the first VLAN, responsive to the authentication request comprises receiving user identification data from the unauthorized computing device based on information captured by the network login page.

38. (Currently amended) The computer-readable medium of claim 37, wherein directing the unauthorized computing device to the network login page for authentication comprises:

responding to the unauthorized computing device with a redirect to a Uniform Resource Locator (URL) address for the network login page.

39. (Previously presented) The computer-readable medium of claim 35, further comprising:

sending the authentication credentials to a Remote Authentication Dial-In User Service (RADIUS) compatible authentication server; and

receiving an indication from the RADIUS compatible authentication server that the authentication credentials are authentic and that a user associated with the authentication credentials is authorized to access the network.

40. (Currently amended) A system comprising:

means for receiving a connection request from an unauthorized computing device at a first port of a packet forwarder, the unauthorized computing device requesting access to a network communicably interfaced with a second port of the packet forwarder;

means for blocking all data packets received at the first port of the packet forwarder from accessing the network;

means for issuing the unauthorized computing device a first Internet Protocol (IP) address assigned to a first Virtual Local Area Network (VLAN) ~~communicably interfaced with~~ operating within the packet forwarder and associated with the first port, wherein the first VLAN does not provide access to the network communicably interfaced with the packet forwarder via the second port, and wherein the packet forwarder blocks the data packets in the first VLAN from reaching ~~and is isolated from~~ a permanent VLAN that provides access to the network, the permanent VLAN operating within the network and associated with the second port of the packet forwarder and not the first port of the packet forwarder;

means for sending the unauthorized computing device an authentication request through the first port of the packet forwarder via the first VLAN based on the first IP address, responsive to the connection request;

means for authorizing the computing device based on satisfactory ~~receiving~~ authentication credentials received from the computing device through the first port of the packet forwarder via the first VLAN, responsive to the authentication request;

means for issuing the authorized computing device a replacement IP address assigned to the permanent VLAN for communication with the network and associating the first port of the network forwarder with the permanent VLAN; and ~~, responsive to receiving satisfactory authentication credentials from the computing device; and~~

means for forwarding ~~network~~ the data packets ~~between the~~ received from the authorized computing device at the first port of the packet forwarder to ~~and~~ the network via the second port of the packet forwarder using ~~over~~ the permanent VLAN based on the replacement IP address assigned to the authorized computing device.

41. (Currently amended) The system ~~computer-readable medium~~ of claim 40, wherein receiving the connection request from the unauthorized computing device requesting access to the network comprises:

means for intercepting a request from the unauthorized computing device for a web page.

42. (Currently amended) The system of claim 40, wherein:

sending the unauthorized computing device the authentication request comprises means for directing the unauthorized computing device to a network login page for authentication, the network login page accessible on the first VLAN; and wherein

receiving the authentication credentials from the unauthorized computing device via the first VLAN, responsive to the authentication request comprises means for receiving a user identification card from the unauthorized computing device based on information captured by the network login page.

43. (Currently amended) The system of claim 42, wherein directing the unauthorized computing device to the network login page for authentication comprises:

means for responding to the unauthorized computing device with a redirect to a Uniform Resource Locator (URL) address for the network login page.

44. (Previously presented) The system of claim 40, further comprising:

means for sending the authentication credentials to a Remote Authentication Dial-In User Service (RADIUS) compatible authentication server; and

means for receiving an indication from the RADIUS compatible authentication server that the authentication credentials are authentic and that a user associated with the authentication credentials is authorized to access the network.

45. (New) The method of claim 26, wherein the authentication credentials received from the unauthorized computing device comprise user-specific credentials which are independent of hardware associated with the unauthorized computing device; and wherein

authorizing the unauthorized computing device based on satisfactory authentication credentials received from the unauthorized computing device comprises authorizing a user of the unauthorized computing device based on the user-specific credentials.